The XL-Algorithm and a Conjecture from Commutative Algebra

Claus Diem

Institute for Experimental Mathematics, University of Duisburg-Essen
Essen, Germany

Abstract. The "XL-algorithm" is a computational method to solve overdetermined systems of polynomial equations which is based on a generalization of the well-known method of linearization; it was introduced to cryptology at Eurocrypt 2000.
In this paper, we prove upper bounds on the dimensions of the spaces of equations in the XL-algorithm. These upper bounds provide strong evidence that for any fixed finite field K and any fixed $c \in \mathbb{N}$ the median of the running times of the original XL-algorithm applied to systems of $m = n+c$ quadratic equations in n variables over K which have a solution in K is not subexponential in n. In contrast to this, in the introduction of the original paper on XL, the authors claimed to "provide strong theoretical and practical evidence that the expected running time of this technique is [...] subexponential if m exceeds n by a small number".
More precise upper bounds on the dimensions of the spaces of equations in the XL-algorithm can be obtained if one assumes a standard conjecture from commutative algebra. We state the conjecture and discuss implications on the XL-algorithm.

Keywords. Cryptanalysis, algebraic attacks, overdetermined systems of polynomial equations, extended linearization, Fröberg's Conjecture

1 Motivation and introduction

The security of many cryptographic systems would be jeopardized if one could solve certain types of systems of polynomial equations over finite fields. For example, it has been pointed out in [8] that one can with a high probability recover an AES-128 key from one AES-128 plaintext-ciphertext pair if one can solve certain systems with 1600 variables and 8000 quadratic equations over $\mathbb{F}_2$, and it has been pointed out in [14] that one can achieve the same goal if one can solve certain systems with 3986 variables and 3840 (sparse) quadratic equations as well as 1408 linear equations over $\mathbb{F}_{2^8}$.

Of particular importance for cryptological applications are so-called *overdetermined* (or *overdefined*) systems of quadratic equations as for example the ones we just mentioned. Let us consider a system of quadratic polynomial equations

$$f_1(X_1, \ldots, X_n) = 0\,,\ \ldots\ ,\ f_m(X_1, \ldots, X_n) = 0\ \ , \tag{1}$$

where the f_j are polynomials in n indeterminates $X_1, \ldots, X_n$ over an "effective" field K (the field being finite in the cryptological applications). We say that the system is *overdetermined* if the dimension of the K-vector space generated by the f_j is greater than n.

In [7], Courtois, Klimov, Patarin and Shamir propose a computational method called *eXtended Linearization (XL)* or *XL-algorithm* to solve such systems of polynomial equations (see the next section for a description of the method). In the same paper certain heuristics on the running time of this method are stated. These heuristics have subsequently been criticized by Moh ([13]) as being too optimistic, and in Sect. 4 of [13], the method is analyzed with heuristic upper bounds on the dimensions on the spaces of equations in the XL-algorithm. As however the assumptions on which the heuristic in [13, Sect. 4] relies are not very precisely stated, the question whether this heuristic or the original heuristic is more credible remained an open problem among cryptologists. In a recent work by Chen and Yang ([4]), the heuristic of [13, Sect. 4] is stated as a special case of a theorem ([4, Theorem 2]).[1] However, the proof of [4, Theorem 2] (and of [4, Theorem 7]) has some serious flaws.

The main purpose of this paper is to show that under the assumption of a widely believed conjecture of commutative algebra, one can indeed derive the non-trivial upper bounds on the dimensions of the spaces of equations in the XL-algorithm conjectured by Moh and stated in [4, Corollary 6, 1] (see Theorem 1 in Sect. 5 for a more general statement). Moreover, we state upper bounds on the dimensions of the spaces of equations in the original XL-algorithm which can be proven without the assumption of this conjecture. These upper bounds provide strong evidence that for any fixed finite field K and any fixed $c \in \mathbb{N}$ the median of the running times of the original XL-algorithm applied to systems of $m = n + c$ quadratic equations in n variables over K which have a solution in K is not subexponential in n (see the next section for details).

2 The XL-algorithm and our analysis

Let us fix the system of quadratic equations (1) which we assume to have a solution in K and some $D \in \mathbb{N}$. The main idea of the XL-algorithm is to try to solve (1) by linearization of the system of all polynomial equations

$$\prod_{\ell=1}^{k} X_{i_\ell} \cdot f_j(X_1, \ldots, X_n) = 0 \ , \tag{2}$$

where $k \leq D - 2$.

Let U_D be K-vector space generated by the polynomials $\prod_{\ell=1}^{k} X_{i_\ell} \cdot f_j$ with $k \leq D - 2$.

According to [7, Definition 1], the XL-algorithm is as follows. (Except for changes in the notation, the description is verbatim.)

[1] Theorem 2 of [4] is equivalent to the heuristics of [13] if $D < q$ as can be seen by expanding the polynomial in item 1 of Corollary 6 in [4].

The XL-algorithm. *Execute the following steps:*

1. Multiply: *Generate all the products* $\prod_{\ell=1}^{k} X_{i_\ell} \cdot f_j \in U_D$ *with* $k \leq D-2$.
2. Linearize: *Consider each monomial in* X_i *of degree* $\leq D$ *as an independent variable*[2] *and perform Gaussian elimination on the equation obtained in* 1. *The ordering on the monomials must be such that all the terms containing one [specific] variable (say* X_1*) are eliminated last.*
3. Solve: *Assume that step 2 yields at least one univariate equation in the powers of* X_1. *Solve this equation over the finite fields (e.g. with Berlekamp's algorithm).*[3,4]
4. Repeat: *Simplify the equations and repeat the process to find the values of the other variables.*

Remark 1. In the description of the method in [7], it seems that D is fixed beforehand. As the authors do however not say how D should be determined, it seems to be reasonable to assume that the authors of [7] had in mind that D is in fact a variable which is small (e.g. 2) in the beginning, and that the the XL-algorithm goes to Step 1 with an incremented D whenever in Step 3 no univariate equation in X_1 with a solution in K is found.

Remark 2. In an "extended version" ([6]) of [7], the description of the method is the same as the one in [7] (and the one we present here) except that the authors have inserted the sentence "In all the following notations we suppose the powers of variables taken over K, i.e. reduced modulo q to the range $1, \ldots, q-1$ because of the equation $a^q = a$ of the finite field K." after the third paragraph of Sect. 3. (But the field is not assumed to be finite in the second paragraph of Sect. 3 and the number q is not mentioned before.) Apart from this insertion, there is no substantial difference between Sect. 3 to 7 of [7] and of [6]. Of course, if one identifies the monomials $\prod_{\ell=1}^{k} X_{i_\ell}$ and $X^q \cdot \prod_{\ell=1}^{k} X_{i_\ell}$ the method becomes much faster if q, the field size, is small, $q = 2, 3, 4, 5$ say. According to the way the heuristics in Sect. 6 of [7] and [6] were conducted, this identification was however *not* made in the heuristic analysis of [7] and [6].

Definition 1. *We call the above computational method the* original XL-algorithm. *The variant introduced in [6] is called* reduced XL-algorithm.

Remark 3. Whereas the original XL-algorithm should only be applied to overdetermined systems of (quadratic) polynomial equations, if the field is finite and not too large, it makes sense to apply the reduced XL-algorithm to any system of (quadratic) polynomial equations.

---

[2] The authors of [7] obviously mean that each monomial of degree $\leq D$ should be considered as a new variable.

[3] Note however that according to the second paragraph in [7, Sect. 3], the ground field is not necessarily finite.

[4] It should be avoided to repeatedly select univariate polynomial equations which have more than one solution in K. Moreover, if a univariate polynomial equation is found which does not have a solution in K, the method should terminate and output "unsolvable".

Remark 4. Neither of the two computational methods terminates for every input (even if they are only applied to overdetermined systems which have a solution in K); thus in contrast to their names, they are not algorithms (not even randomized algorithms) in the usual sense (cf. [11, Chapter 1, 1.1]).

As we will see in the next section, there is a strong connection between the original and the reduced XL-algorithm (see Proposition 1). Because of this connection, one can use an analysis of (a generalization of) the original XL-algorithm to analyze also the reduced XL-algorithm (see Theorem 1 and Corollary 1). In order to state the main ideas of our analysis and to compare our results with the conjectures of [7], in this section, we concentrate on the original XL-algorithm.

For $D \in \mathbb{N}$, let $K[X_1, \ldots, X_n]_{\leq D}$ be the K-vector space of polynomials in $X_1, \ldots, X_n$ of (total) degree $\leq D$, and let

$$\chi(D) := \dim_K(K[X_1, \ldots, X_n]_{\leq D}) - \dim_K(U_D) \ . \tag{3}$$

One can surely obtain a non-trivial univariate polynomial by (Gaussian) elimination on (2) if $\chi(D) \leq D$. (This is because the K-vector space $K[X_1]_{\leq D}$ has dimension $D+1$, thus if $\chi(D) \leq D$, then $\dim_K(U_D) + \dim_K(K[X_1]_{\leq D}) > \dim_K(K[X_1, \ldots, X_n]_{\leq D})$, and this implies that $U_D \cap K[X_1]_{\leq D} \neq \{0\}$.) In order to analyze the running time of the XL-algorithm, it is of greatest importance to study the question for which D one can expect this condition to hold (if such a D exists at all). We thus define $D_{\min}$ be the minimal D with $\chi(D) \leq D$ (if no such D exists, we set $D_{\min} = \infty$).

The starting point for our analysis of the XL-algorithm is the interpretation of the original XL-algorithm via the theory of *homogeneous* polynomial ideals pointed out by Moh ([13]). This interpretation opens the door for the usage of well-established methods from commutative algebra – the keywords are Hilbert Theory, Hilbert functions, Hilbert series and Hilbert polynomials.

A crucial observation is that in order to derive lower bounds on $\chi(D)$ (i.e. upper bounds on $\dim_K(U_D)$) it suffices to study the dimensions of the homogeneous parts of algebras defined by *generic* systems of homogeneous polynomials. (This notion will be made precise in Sect. 4.) For $m \leq n+1$, these dimensions are known, and this information suffices to prove that for $m = n + c, c \geq 1$,

$$D_{\min} \geq \frac{n}{\sqrt{c-1}+1} \tag{4}$$

(see Proposition 6.) In contrast to this inequality, it was suggested in [7, Sect. 6.4] that "even for small values of c", $c \geq 2$, one has

$$D_{\min} \approx \sqrt{n} \ . \tag{5}$$

Let us fix the field K and $c \geq 2$ and study the asymptotic behavior of the running time of the original XL-algorithm for $n \longrightarrow \infty$ (and $m = n + c$): If (5) was true, the XL-algorithm in [7] would have a running time (in field operations) which is *subexponential* in n. (This hope was expressed at the end of Sect. 6.1 of [7] as well as at the end of the introduction of [7].) However by (4), the running time of all instances for which $U_D \cap K[X_1]_{\leq D} = \{0\}$ for all $D < D_{\min}$ is *not subexponential* in n.

If K is a finite field and $\#K$ and n are not "too small" it seems very reasonable to expect: Under all systems (1) which have a solution in K, the portion of systems for which $U_D \cap K[X_1]_{\leq D} \neq \{0\}$ for some $D < D_{\min}$ is negligible. This suggests that for any fixed $c \geq 1$ the median of the running times of the original XL-algorithm applied to systems of $m = n + c$ quadratic equations in n variables over K which have a solution in K is not subexponential in n. The hope stated at the end of Sect. 1 of [7] that "the expected running time of this technique is ... subexponential if m exceeds n by a small number" should be abandoned.

For $c \geq 3$, much more precise lower bounds on $D_{\min}$ then the ones in (4) can be obtained if one assumes a certain conjecture which implies what the dimensions of homogeneous parts of algebras defined by generic systems of homogeneous polynomials should be (see Sect. 5). This conjecture – which is now approximately 20 years old – states that certain linear maps are either injective or surjective, that is, they have maximal rank. Because of this, we speak of the *maximal rank conjecture (MR-conjecture).*

3 A generalization of the original and the reduced XL-algorithm

The original as well as the reduced XL-algorithm of can easily be generalized to more general than quadratic systems of polynomial equations (see also [5, Sect. 2]).

For these generalizations, we start off with a system of m polynomial equations

$$f_1(X_1, \ldots, X_n) = 0, \ \ldots \ , f_m(X_1, \ldots, X_n) = 0 \ . \tag{6}$$

The generalization of the original XL-algorithm works just as the original XL-algorithm stated in the previous section with the difference that for some $D \in \mathbb{N}$, one applies Gaussian elimination to the linearized system of all polynomial equations

$$\prod_{\ell=1}^{k} X_{i_\ell} \cdot f_j(X_1, \ldots, X_n) = 0 \ , \tag{7}$$

where $k + \deg(f_j) \leq D$.

Clearly, the reduced XL-algorithm can be generalized in a similar manner. From now on, we refer to these generalizations also as the "original" and the "reduced" XL-algorithm.

Let us fix the following *notations.*

– As in the previous section, let

$$U_D := \langle \textstyle\prod_{\ell=1}^{k} X_{i_\ell} \cdot f_j(X_1, \ldots, X_n) \text{ with } k \leq D - \deg(f_j) \rangle_K \tag{8}$$

– and

$$\chi(D) := \dim_K(K[X_1, \ldots, X_n]_{\leq D}) - \dim_K(U_D)\ . \tag{9}$$

Let $K = \mathbb{F}_q$.

– If $f \in K[X_1, \ldots, X_n]_{\leq D}$, we denote by f^{red} the "reduction" of f, i.e. f^{red} is the polynomial obtained by maximally reducing all exponents in the monomials according to the relations $\prod_{\ell=1}^{k} X_{i_\ell} - X_i^q \cdot \prod_{\ell=1}^{k} X_{i_\ell} = 0$. Note that $(\ldots)^{\text{red}}$ is a homomorphism of K-vector spaces and that $(U_D)^{\text{red}} \leq (K[X_1, \ldots, X_n]_{\leq D})^{\text{red}}$ is the space of equations generated in the reduced XL-algorithm.
– In order to analyze the reduced XL-algorithm, we set

$$\chi^{\text{red}}(D) := \dim_K((K[X_1, \ldots, X_n]_{\leq D})^{\text{red}}) - \dim_K((U_D)^{\text{red}})\ . \tag{10}$$

– Let $\tilde{U}_D$ be defined just as U_D with respect to the system of $m+n$ polynomials $f_1, \ldots, f_m, X_1^q - X_1, \ldots, X_n^q - X_n$, and let $\tilde{\chi}(D)$ be defined as $\chi(D)$ with respect to $\tilde{U}_D$.

The proof of the following proposition can be found in Appendix A.

Proposition 1. *We have* $\chi^{\text{red}}(D) = \tilde{\chi}(D)$.

Because of this proposition, the results on the original XL-algorithm can easily be carried over to the reduced XL-algorithm. What remains is to derive non-trivial lower bounds on $\chi(D)$.

4 The XL-algorithm and Hilbert Theory

In the following discussion, we assume that the reader is familiar with basic notions of commutative algebra as can for example be found in the first three chapters of [1].

As mentioned in Sect. 2, our analysis of the XL-algorithm relies on an interpretation via homogeneous polynomial ideals. The main idea is to consider (for some field K, some $n \in \mathbb{N}$ and some $D \in \mathbb{N}$) the homogeneous polynomials of degree D in $n+1$ variables instead of the polynomials of degree $\leq D$ in n variables.

Let K be an arbitrary field, $n \in \mathbb{N}$, and let $f_1, \ldots, f_n \in K[X_1, \ldots, X_n]$. We use the notations of the previous sections, and additionally we denote by $K[X_0, \ldots, X_n]_D$ the K-vector space of all homogeneous polynomials of degree D. More generally, for any positively graded $K[X_0, \ldots, X_n]$-module M, we denote the homogeneous part of degree D of M by M_D.

Let $F_j \in K[X_0, \ldots, X_n]$ be the homogenization of f_j, that is, F_j is the unique homogeneous polynomial in $K[X_0, \ldots, X_n]$ of the same degree as f_j with $F_j(1, X_1, \ldots, X_n) = f_j(X_1, \ldots, X_n)$.

Let

$$\Phi : K[X_1, \ldots, X_n]_{\leq D} \longrightarrow K[X_0, \ldots, X_n]_D$$

be the "degree D homogenization map", that is, the K-linear map given by

$$\prod_{\ell=1}^{k} X_{i_\ell} \mapsto X_0^{D-k} \prod_{\ell=1}^{k} X_{i_\ell} \quad .$$

Then under the isomorphism Φ, the K-vector space U_D corresponds to

$$\langle \prod_{\ell=1}^{k} X_{i_\ell} \cdot F_j(X_0, X_1, \ldots, X_n) \text{ with } k = D - \deg(F_j) \rangle_K \quad ,$$

where the products are taken over the variables $X_0, \ldots, X_n$. This space is nothing but the D^{th} homogeneous component of the homogeneous ideal

$$I := (F_1, \ldots, F_m) \lhd K[X_0, \ldots, X_n] \quad ,$$

denoted I_D. We have

$$\begin{aligned} \chi(D) &\stackrel{\text{Def}}{=} \dim_K(K[X_1, \ldots, X_n]_{\leq D}) - \dim_K(U_D) \\ &= \dim_K(K[X_0, \ldots, X_n]_D) - \dim_K(I_D) \\ &= \dim_K(K[X_0, \ldots, X_n]_D / I_D) \\ &= \dim_K((K[X_0, \ldots, X_n]/I)_D) \quad . \end{aligned} \tag{11}$$

Let $R := K[X_0, \ldots, X_n]$. Recall the following definitions (see e.g. [16, Sect. 1]).

Definition 2. *Let $M = \bigoplus_{i \in \mathbb{N}_0} M_i$ be any finitely generated positively graded R-module. Then the function*

$$\chi_M : \mathbb{N}_0 \longrightarrow \mathbb{N}_0, \quad \chi_M(i) := \dim_K(M_i)$$

is called the Hilbert function *of M.*

The power series with integer coefficients

$$H_M := \sum_{i \in \mathbb{N}_0} \chi_M(i) T^i$$

is called the Hilbert series *of M.*

Note that the above equation (11) states that

$$\chi(D) = \chi_{R/I}(D) \quad \text{for all } D \in \mathbb{N} \quad . \tag{12}$$

Let us denote by $X^{\underline{i}}$ the monomial corresponding to the multiindex $\underline{i} \in \mathbb{N}_0^{\{0,\ldots,n\}}$. The following definition can be found in [10].

Definition 3. *A form (i.e. a homogeneous polynomial) $G = \sum_{\underline{i}} a_{\underline{i}} X^{\underline{i}} \in R$ of degree d is* generic *if all monomials of degree d in R have coefficients $a_{\underline{i}}$ in G, and these coefficients are algebraically independent over the prime field of K.*

A generic system of forms *is a system of generic forms $G_j = \sum_{\underline{i}} a_{\underline{i}}^{(j)} X^{\underline{i}}$ as above (not necessarily of the same degree) such that all $a_{\underline{i}}^{(j)}$ are algebraically independent over the prime field of K. An ideal I generated by a generic system of forms is called* generic, *and so is the R-algebra R/I.*

Lemma and Definition 4. *The Hilbert series of an ideal generated by a generic system $G_1, \ldots, G_m$ of forms of degrees $d_1, \ldots, d_m$ depends only on the characteristic of the field, the number n and the tuple of numbers $(d_1, \ldots, d_m)$. If the characteristic of the field is 0, we speak of* the generic Hilbert series *of type $(n+1; m; d_1, \ldots, d_m)$.*

Proof. Let K and L be two fields over the same prime field F, and let $G_1, \ldots, G_m \in K[X_0, \ldots, X_n], G'_1, \ldots, G'_m \in L[X_0, \ldots, X_n]$ be two generic systems of forms such that $\deg(G_j) = \deg(G'_j)$ for all j. Let $G_j = \sum_{\underline{i}} a^{(j)}_{\underline{i}} X^{\underline{i}}$, $G'_j = \sum_{\underline{i}} a'^{(j)}_{\underline{i}} X^{\underline{i}}$. Let k and l respectively be the subfields of K and L generated by the coefficients of G_j and G'_j over F. Then there exists a (unique) isomorphism between k and l under which $a^{(j)}_i$ corresponds to $a'^{(j)}_i$. We thus have for all $D \in \mathbb{N}_0$

$$\begin{gathered}\chi_{K[X_0,\ldots X_n]/(G_1,\ldots,G_m)}(D) = \dim_K((K[X_0, \ldots X_n]/(G_1, \ldots, G_m))_D) = \\ \dim_k((k[X_0, \ldots X_n]/(G_1, \ldots, G_m))_D) = \\ \dim_l((l[X_0, \ldots X_n]/(G'_1, \ldots, G'_m))_D) = \\ \dim_L((L[X_0, \ldots X_n]/(G'_1, \ldots, G'_m))_D) = \chi_{L[X_0,\ldots X_n]/(G'_1,\ldots,G'_m)}(D) \enspace .\end{gathered}$$

$\square$

Together with (12), the following proposition is crucial for our analysis of the XL-algorithm.

Proposition 2. *Let K be any field (of any characteristic), and let $F_1, \ldots, F_m \in R = K[X_0, \ldots, X_n]$ be forms of degree $d_1, \ldots, d_m$ (not necessarily generic). Let H_g be the generic Hilbert series of type $(n+1; m; d_1, \ldots, d_m)$. Let $I := (F_1, \ldots, F_m) \lhd K[X_0, \ldots, X_n]$. Then we have the coefficient-wise inequality*

$$H_{R/I} \geq H_g \enspace .$$

This proposition seems to be well-known in commutative algebra (see e.g. Sect. 4 of [16]); for the lack of a suitable reference we include the proof in Appendix B.

Because of (12) and this proposition the task is now to study generic Hilbert series. The following proposition is a well-known statement from commutative algebra.

Proposition 3. *Let $m \leq n+1$, and let $G_1, \ldots, G_{m-1}, G_m = G$ be a generic system of forms in $R = K[X_0, \ldots, X_n]$, where G has degree d. Let $J := (G_1, \ldots, G_{m-1}) \lhd R$. Then for all $D \in \mathbb{N}_0$ the multiplication map*

$$G\cdot : (R/J)_D \longrightarrow (R/J)_{D+d},\ \overline{F} \mapsto G \cdot \overline{F}$$

is injective, in particular we have a short exact sequence

$$0 \longrightarrow (R/J)_D \xrightarrow{G\cdot} (R/J)_{D+d} \longrightarrow (R/(J,G))_{D+d} \longrightarrow 0 \enspace .$$

(Here by (J, G) we denote the ideal of R generated by J and G.)

Indeed, this proposition is nothing but a reformulation of the well-known statement that a generic system of forms in $K[X_0, \dots, X_n]$ with at most $n+1$ elements forms a regular sequence (cf. [16, Sect. 4], Page 318). (The fact that a generic system of forms is a regular sequence can be seen as follows: By Lemma 3 in Appendix B, it suffices to prove that for all $(d_1, \dots, d_{n+1}) \in \mathbb{N}^{n+1}$ there exist some forms $F_1, \dots, F_{n+1} \in R$ of degrees $d_1, \dots, d_{n+1}$ which form a regular sequence, and by [12, Theorem 16.1], the forms $X_0^{d_1}, \dots, X_n^{d_{n+1}}$ do form a regular sequence.)

Note that the Hilbert series of $R = K[X_0, \dots, X_n]$ is

$$H_R = \sum_i \binom{n+i}{i} T^i = \frac{1}{(1-T)^{n+1}} \tag{13}$$

(see e.g. [16, Sect. 1]). Proposition 3 and (13) imply by induction on m:

Proposition 4. *Let $m \leq n+1$, and let $G_1, \dots, G_m$ be a generic system of forms of degrees $d_1, \dots, d_m$ in R. Then the Hilbert series of $R/(G_1, \dots, G_m)$ is*

$$\frac{\prod_{j=1}^{m} (1 - T^{d_j})}{(1-T)^{n+1}} \ .$$

For simplicity we now concentrate until the end of this section on the case of *quadratic* equations.

Proposition 5. *Let $m = n + c$ for some $c \geq 1$. Let $F_1, \dots, F_m$ be quadratic forms in $R = K[X_0, \dots, X_n]$. Then the Hilbert series of $R/(F_1, \dots, F_m)$ is coefficient-wise greater-or-equal*

$$(1 - (c-1)T^2)(1+T)^{n+1} \ .$$

Proof. By Proposition 2 we only have to prove that the generic Hilbert series of type $(n+1; m; 2, \dots, 2)$ is coefficient-wise greater-or-equal $(1-(c-1)T^2)(1+T)^{n+1}$.

So let K be a field of characteristic 0, let $R = K[X_0, \dots, X_n]$, and let $G_1, \dots, G_m$ be a generic system of quadratic forms in R. (The assumption on the characteristic is not necessary for the following argument.) Let $R' := R/(G_1, \dots, G_{n+1})$, and let I' be the ideal generated by $G_{n+2}, \dots, G_m$ in R'. Note that by the above proposition, the Hilbert series of R' is $(1+T)^{n+1}$. We have $R/(G_1, \dots, G_m) \simeq R'/I'$, thus

$$\chi_{R/(G_1,\dots,G_m)}(D) = \chi_{R'/(G_{n+2},\dots,G_m)}(D) = \dim_K(R'_D) - \dim_K(I'_D) \ .$$

Now, for $D \geq 2$, $I'_D = \sum_{j=n+2}^{m} G_j \cdot R'_{D-2}$, where by definition $G_j \cdot R'_{D-2}$ is the image of R'_{D-2} under the multiplication map $G_j \cdot : R'_{D-2} \longrightarrow R'_D$. It follows that

$$\dim_K(I'_D) \leq (m-n-1) \dim_K(R'_{D-2}) \ .$$

All in all, we have

$$\chi_{R/(G_1,\ldots,G_m)}(D) \geq \chi_{R'}(D) - (c-1)\chi_{R'}(D-2) \ ,$$

thus

$$H_{R/(G_1,\ldots,G_m)} \geq H_{R'} - (c-1)T^2 H_{R'} = (1-(c-1)T^2)(1+T)^{n+1} \ .$$

Proposition 6. *Let K be any field, let $m = n+c$ with $c \geq 1$, let $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ be quadratic polynomials, and as in Sect. 2, let $D_{\min}$ be the minimal D with $\chi(D) \leq D$, where $\chi(D)$ is defined as above with respect to these polynomials. Then*

$$D_{\min} \geq \frac{n}{\sqrt{c-1}+1} \ .$$

Sketch of the Proof. Let $c \geq 1$, $m = n+c$, $f_1, \ldots, f_m$ and $\chi(D)$ be as in the proposition. By (12) and the above proposition, we have

$$\chi(D) \geq (\frac{(n-D+2)(n-D+3)}{(D-1)D} - (c-1)) \cdot \binom{n+1}{D-2}$$

for all $D \geq 2$. The proposition follows from the statement that $(\frac{(n-D+2)(n-D+3)}{(D-1)D} - (c-1)) \cdot \binom{n+1}{D-2} > D$ for all $D < \frac{n}{\sqrt{c-1}+1}$. We only show the slightly weaker statement that $\frac{(n-D+2)(n-D+3)}{(D-1)D} - (c-1) > 0$ for all $D < \frac{n}{\sqrt{c-1}+1}$.

Let $D < \frac{n}{\sqrt{c-1}+1}$. Then $D\sqrt{c-1} + D < n$, thus $D^2(c-1) < (n-D)^2$. This implies that $(D-1)D(c-1) < (n-D+2)(n-D+3)$, i.e. $\frac{(n-D+2)(n-D+3)}{(D-1)D} - (c-1) > 0$. □

Remark 5. For an application of the XL-algorithm to a system with $m = n$ quadratic equations, one can easily see with Propositions 2 and 4 and (12) that one always has $\chi(D) \geq 2^n$, and for $m = n+1$ quadratic equations, one has $D_{\min} \geq n+1$. Both these results are consistent with conjectures in [7].

5 The maximal rank conjecture

The *maximal rank conjecture (MR-conjecture)* which we now state can be thought to be a (potential) generalization of Proposition 3.

Conjecture. Let K be a field of characteristic 0, and let $G_1, \ldots, G_{m-1}, G_m = G$ be a generic system of forms in $R = K[X_0, \ldots, X_n]$, where G has degree d. Let $J := (G_1, \ldots, G_{m-1}) \lhd R$. Then for all $D \in \mathbb{N}_0$ the multiplication map

$$G\cdot\ : (R/J)_D \longrightarrow (R/J)_{D+d},\ \overline{F} \mapsto G \cdot \overline{F}$$

has *maximal rank*, that is it is injective if $\dim_K((R/J)_D) \leq \dim_K((R/J)_{D+d})$ and it is surjective if $\dim_K((R/J)_D) \geq \dim_K((R/J)_{D+d})$.

This conjecture – which is also known under the name "Fröberg's Conjecture" – can (in an equivalent formulation) be found in [10]. It is also stated in Sect. 4

of the informative overview article [16]. (Note however that the formulations at the beginning of Sect. 4 of [16] are a bit vague.) Interesting facts about this and related conjectures can be found in [15].

The conjecture is known to hold if one of the following five conditions is satisfied: $m \leq n+1$ (see Proposition 3), $n = 1, n = 2$, $m = n+2$, $D = \min_j\{\deg(G_j)\} + 1$ (see [10, 3.2.] and the citations in [16, Sect. 4]).

The conjecture is equivalent to the statement that

$$\chi_{R/(J,G)}(D) = \max\{\chi_{R/J}(D) - \chi_{R/J}(D-d)\,,\, 0\}$$

as one can easily see (cf. [16, Sect. 4]). (Here, we set $\chi_{R/J}(i) = 0$ for $i < 0$.)

Obviously, if $\chi_{R/(J,G)}(D) = 0$, then $\chi_{R/(J,G)}(D') = 0$ for all $D' > D$. Using this fact, the conjecture can be reformulated via Hilbert series as:

$$H_{R/(I,G)} = |(1 - T^d)H_{R/I}| \ , \tag{14}$$

where for some power series $p(T)$ with integer coefficients, $|p(T)|$ denotes the power series $q(T) = \sum_i q_i T^i$, where

$$\begin{aligned} q_i = p_i &\text{ if } p_j > 0 \text{ for all } j \leq i \\ 0 &\text{ if } p_j \leq 0 \text{ for some } j \leq i \ . \end{aligned}$$

Assumption. *From now on, we assume that the maximal rank conjecture is valid.*

Let K be a field of characteristic 0, let $G_1, \ldots, G_m$ be a generic system of forms in R, and let $d_j := \deg(G_j)$. Let $I := (G_1, \ldots, G_m)$. Using (13), (14) and Lemma 5 in Appendix C, we have

$$H_{R/I} = \left| \frac{\prod_{j=1}^m (1 - T^{d_j})}{(1 - T)^{n+1}} \right| \ . \tag{15}$$

Definition 5. *(see [16]) We call the right-hand side of the above equation the* expected Hilbert series *of a generic algebra of type $(n+1; m; d_1, \ldots, d_m)$.*

Proposition 2 implies:

Proposition 7. *Let K be any field (of any characteristic), and let $F_1, \ldots, F_m \in R = K[X_0, \ldots, X_n]$ be forms of degree $d_1, \ldots, d_m$ (not necessarily generic). Let H_e be the corresponding expected Hilbert series. Let $I := (F_1, \ldots, F_m)$. Then we have the coefficient-wise inequality*

$$H_{R/I} \geq H_e \ .$$

Together with (12), this proposition has the following implication for the original XL-algorithm.

Theorem 1. *Let K be any field, let $f_1, \ldots, f_m$ be non-trivial polynomials in $K[X_1, \ldots, X_n]$ with degrees $d_1, \ldots, d_m$. Let $D \in \mathbb{N}$, and let $\chi(D)$ be defined as in (9). Then $\chi(D)$ is greater-or-equal to the D^{th} term of the expected Hilbert series of a generic algebra of type $(n+1; m; d_1, \ldots, d_m)$.*

By Proposition 1, this theorem has the following corollary which can be used to analyze the reduced XL-algorithm.

Corollary 1. *With the notations of the theorem, let $K = \mathbb{F}_q$, and let $\chi^{\mathrm{red}}(D)$ be defined as is (10). Then $\chi^{\mathrm{red}}(D)$ is greater-or-equal to the D^{th} term of the expected Hilbert series of a generic algebra of type $(n+1; m+n; d_1, \ldots, d_m, q, \ldots, q)$.*

Remark 6. Let $D_{n,m}$ be the degree of the expected Hilbert series of a generic algebra of type $(n+1; m; 2, \ldots, 2)$. One can use the methods presented in [2, Sect. 5] to study asymptotic behaviors of $D_{n,m}$. A corresponding study is carried out in [3]. One obtains $D_{n,n+c} \sim \frac{n}{2}$ for any fixed $c \geq 2$ and $n \longrightarrow \infty$. (More precise results for various small c can also be found in [3].) For a fixed $\alpha > 1$, a reformulation of a result in [3] gives $D_{n,\alpha n} \sim (\alpha - \sqrt{\alpha^2 - \alpha} - \frac{1}{2}) \cdot n$ for $n \longrightarrow \infty$. For example, one has $D_{n,2n} \sim C \cdot n$ with $C = \frac{3}{2} - \sqrt{2} \approx 0.0858$ (which is consistent with the "Comparison with $2n$ equations over $\mathbb{Q}$" on page 13 of [2]).

Acknowledgment

I thank G. Böckle, T. Bröcker, C. Cid, A. Conca, G. Frey, S. Galbraith, J. Herzog, J. Scholten, A. Wiebe and B.-Y. Yang for discussions. I am particularly in debt to J. Herzog and A. Wiebe for pointing out the "maximal rank conjecture" to me.

Support by the IST Programme "Ecrypt" of the European Union is gratefully acknowledged.

References

[1] M. Atiyah and I. Macdonald. *Introduction to Commutative Algebra.* Addison-Wesley, Reading, 1969.

[2] M. Bardet, J.-C. Faugère, and B. Salvy. Complexity of Gröbner basis computations for Semi-regular Overdetermined sequences over $\mathbb{F}_2$ with solutions in $\mathbb{F}_2$. INRIA Rapport de recherche No. 5049, 2003.

[3] J.-M. Chen and B.-Y. Yang. All in the XL Familiy: Theory and Practice. manuscript from June 2004.

[4] J.-M. Chen and B.-Y. Yang. Theoretical Analysis of XL over Small Fields. In H. Wang, J. Pieprzyk, V. Varadharajan, editors, *Information Security and Privacy*, volume 3108 of *LNCS*, pages 277-288, Springer-Verlag, Berlin, 2004.

[5] N. Courtois. Higher Order Correlation Attacks, XL algorithm, and Cryptanalysis of Toyocrypt. In P.J. Lee, C.H. Lim, editors, *Advances in Cryptology — ICISC 02*, volume 2587 of *LNCS*, pages 182–199, Springer-Verlag, Berlin, 2002.

[6] N. Courtois, A. Klimov, J. Pararin, and A. Shamir. Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. "extended version", available under http://www.minrank.org/xlfull.pdf (as of August 24, 2004).

[7] N. Courtois, A. Klimov, J. Pararin, and A. Shamir. Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. In B. Preneel, editor, *Advances in Cryptology — EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 392–407. Springer-Verlag, Berlin, 2000.

[8] N. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. In Y. Zheng, editor, *Advances in Cryptology — ASIACRYPT 2002*, volume 2501 of *LNCS*, pages 267–287. Springer-Verlag, Berlin, 2002.

[9] D. Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry.* Springer-Verlag, New York, 1995.

[10] R. Fröberg. An inequality for Hilbert series of graded algebras. *Math. Scand.*, 56:117–144, 1985.

[11] D. Knuth. *The Art of Computer Programming.* Addison-Wesley, Reading, 1973.

[12] H. Matsumura. *Commutative Ring Theory.* Cambridge University Press, Cambridge, UK, 1986.

[13] T. Moh. On the method of "XL" and its inefficiency to TTM. manuscript from January 28, 2000, available under http://eprint.iacr.org/2001/047.

[14] S. Murphy and M.J.B. Robshaw. Essential algebraic structure within the AES. In M. Yung, editor, *Advances in Cryptology — CRYPTO 2002*, pages 1–16, 2002.

[15] K. Pardue. Generic Sequences of Polynomials. manuscript from March 30, 2000.

[16] G. Valla. Problems and Results on Hilbert Polynomials of Graded Algebras. In J. Elas and J. Giral, editors, *Six Lectures on Commutative Algebra*, volume 166 of *Progress in Mathematics.* Birkhäuser, Basel, 1996.

A On the connection between the the original and the reduced XL-algorithm

The purpose of this section is to prove Proposition 1.

As in Proposition 1, let $K = \mathbb{F}_q$. Let

$$V_D := \langle \prod_{\ell=1}^{k} X_{i_\ell} \cdot (X_i^q - X_i) \text{ with } k + q \leq D \rangle_K \leq K[X_1, \ldots, X_n]_{\leq D} \ .$$

Lemma 1. *Let U be any K-vector subspace of $K[X_1, \ldots, X_n]_{\leq D}$. Then we have a short exact sequence*

$$0 \longrightarrow U \cap V_D \longrightarrow U \longrightarrow U^{\mathrm{red}} \longrightarrow 0 \ .$$

Proof. It is obvious that $U \cap V_D$ is contained in the kernel of $(\ldots)^{\mathrm{red}}$. The converse follows from the following lemma. □

Lemma 2. *Let $f \in K[X_1, \ldots, X_n]$. Then there exist polynomials $p_1, \ldots, p_n$ of degree $\leq \deg(f) - q$ with*

$$f = p_1 \cdot (X_1^q - X_1) + \cdots p_n \cdot (X_n^q - X_n) + f^{\mathrm{red}} \ .$$

Proof. By the linearity of $(\ldots)^{\text{red}}$, it suffices to prove the statement for monomials, and for monomials it is obvious by the very definition of $(\ldots)^{\text{red}}$. □

Let us use the definitions of Sect. 3.
We have by Lemma 1

$$(K[X_1,\ldots,X_n]_{\le D})^{\text{red}} \simeq K[X_1,\ldots,X_n]_{\le D}/V_D \ ,$$

$$(U_D)^{\text{red}} \simeq U_D/(U_D \cap V_D) \simeq (U_D + V_D)/V_D \simeq \tilde{U}_D/V_D \ ,$$

thus

$$\begin{aligned}(K[X_1,\ldots,X_n]_{\le D})^{\text{red}}/(U_D)^{\text{red}} &\simeq (K[X_1,\ldots,X_n]_{\le D}/V_D)/(\tilde{U}_D/V_D)\\ &\simeq K[X_1,\ldots,X_n]/\tilde{U}_D \ .\end{aligned}$$

This implies:

$$\begin{aligned}\chi^{\text{red}}(D) &= \dim_K((K[X_1,\ldots,X_n]_{\le D})^{\text{red}}/(U_D)^{\text{red}})\\ &= \dim_K(K[X_1,\ldots,X_n]_{\le D}/\tilde{U}_D) \ = \tilde{\chi}(D) \ .\end{aligned}$$

B Hilbert series of generic and arbitrary algebras

The purpose of this section is to prove Proposition 2. Let us before we come to the proof state two lemmata.

Lemma 3. *Let A be a domain with quotient field Q. Let K be a field and let $\varphi : A \longrightarrow K$ be a homomorphism, and let $\Phi : A[X_0,\ldots,X_n] \longrightarrow K[X_0,\ldots,X_n]$ be the canonical extension of φ. Let $I \lhd A[X_0,\ldots,X_n]$ be a homogeneous ideal (that is, an ideal generated by homogeneous polynomials). Then we have the coefficient-wise inequality*

$$H_{K[X_0,\ldots,X_n]/(\Phi(I))} \ge H_{Q[X_0,\ldots,X_n]/(I)} \ .$$

Proof. Let $D \in \mathbb{N}_0$. The map $\varphi : A \longrightarrow K$ induces a canonical map

$$\begin{aligned}&(A[X_0,\ldots,X_n]/I)_D \longrightarrow (A[X_0,\ldots,X_n]/I)_D \otimes_A K\\ &\quad \simeq (A[X_0,\ldots,X_n]/I \otimes_A K)_D \simeq (K[X_0,\ldots,X_m]/(\Phi(I)))_D.\end{aligned}$$

This implies that

$$\begin{aligned}&\chi_{K[X_0,\ldots,X_n]/(\Phi(I))}(D)\\ &= \dim_K((A[X_0,\ldots,X_n]/I)_D \otimes_A K)\\ &\ge \dim_Q((A[X_0,\ldots,X_n]/I)_D \otimes_A Q) \ \text{ by Lemma 4 below}\\ &= \dim_Q((Q[X_0,\ldots,X_n]/(I))_D)\\ &= \chi_{Q[X_0,\ldots,X_n]/(I)}(D) \ .\end{aligned}$$

Lemma 4. *Let A be a domain with quotient field Q, and let M be a finitely generated A-module. Let K be a field and let $\varphi : A \longrightarrow K$ be a homomorphism. Then*

$$\dim_K(M \otimes_A K) \ge \dim_Q(M \otimes_A Q) \ .$$

Proof. Let $\mathfrak{m}$ be the kernel of φ. Then $M \otimes_A K \simeq M_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} K$ and $M \otimes_A Q \simeq M_{\mathfrak{m}} \otimes_{A_{\mathfrak{m}}} Q$. We can thus assume that A is a local ring with maximal ideal $\mathfrak{m} = \ker(\varphi)$. As the dimension of a vector space is stable under base-change, we can further assume that φ is surjective. Now if $m_1, \ldots, m_r$ form modulo $\mathfrak{m}$ a basis of $M \otimes_A K$ over K then by Nakayama's Lemma ([9, Corollary 4.8]) they generate the A-module M, thus they generate $M \otimes_A Q$ over Q. □

Proof of Proposition 2. We keep the notations of the proposition. The proposition follows from Lemma 3 applied to the multivariate polynomial ring $A = \mathbb{Z}[\{a_{\underline{i}}^{(j)}\}]$, the ideal $I = (G_1, \ldots, G_m)$, where $G_1, \ldots, G_m$ with $G_j = \sum_{\underline{i}} a_{\underline{i}}^{(j)} X^{\underline{i}}$ and $\deg(G_j) = d_j$ is a generic system of forms, and the specialization homomorphism $\varphi : A \longrightarrow K$ sending $a_{\underline{i}}^{(j)}$ to the corresponding coefficient of F_j. (Note that the quotient field of A is $\mathbb{Q}(\{a_{\underline{i}}^{(j)}\})$ which has characteristic 0.) □

C A lemma on power series

The following lemma generalizes [10, Lemma 4]. For the convenience of the reader, we include a proof.

Lemma 5. *Let $p(T)$ be a power series with integer coefficients, let $d \in \mathbb{N}$. Then*

$$|(1 - T^d)p(T)| = |(1 - T^d)|p(T)|| \ .$$

Proof. Note that $((1 - T^d)p(T))_i = p_i$ for $i < d$ and $((1 - T^d)p(T))_i = p_i - p_{i-d}$ for $i \geq d$.

Thus the coefficients whose index is $< d$ of both sides agree. Furthermore, if $p_i < 0$ for some $i < d$, then both sides are equal.

Let us assume that for all $i = 0, \ldots, d - 1$, we have $p_i > 0$.

If now for all i we have $p_i - p_{i-d} > 0$, then we also have $p_i > 0$ for all i as can easily be seen by induction on i. In this case, both sides agree with $(1 - T^d)p(T)$.

Assume that this is not the case and let a be the least natural number for which $p_a - p_{a-d} \leq 0$.

Then for each $i < a$, we have $p_i > 0$ again by induction on i.

There are two cases: Either $p_a > 0$. Then $|p(T)|_a - |p(T)|_{a-d} = p_a - p_{a-d} < 0$ by definition of a. Or $p_a \leq 0$. Then $|p(T)|_a - |p(T)|_{a-d} = -p_{a-d} < 0$.

We conclude that for $i \leq d - 1$, the i-th coefficient of both sides agrees with p_i, for $d < i < a$, the i-th coefficient of both sides agrees with $p_i - p_{i-d}$, and for $i \geq a$, the i-th coefficient of both sides is 0. □

The work described in this paper has been supported in part by the European Commission through the IST Programme under Contract IST-2002-507932 ECRYPT.